NASA CR-144993

AN ENGINEERING TREATISE ON THE CARE II DUAL MODE AND COVERAGE MODELS

FINAL REPORT

April 1976

ER75-4293

PREPARED UNDER

NASA CONTRACT L-[illegible]084A

FOR

NASA LANGLEY RESEARCH CENTER

HAMPTON, VIRGINIA

RAYTHEON COMPANY

EQUIPMENT DEVELOPMENT LABORATORY

SUDBURY, MASSACHUSETTS 01776

ABSTRACT

Under a previous contract with the NASA Langley Research Center (NASA Contract NAS1-12668), Raytheon greatly extended an existing computer program called CARE (Computer Aided Reliability Evaluation), thereby enabling it to calculate the reliability of any dual-mode, spare-switching computer system. The results of that effort are described in "Reliability Model Derivatation of a Fault-Tolerent, Dual, Spare-Switching, Digital Computer System, Final Report", 25 March 1974, (Raytheon Report No. ER74-4108).

The emphasis in that report was on the computer program itself; the mathematical model on which the program was based was briefly outlined but not described in detail. This document supplements this earlier report by providing such a description, presenting some illustrative examples, and examining the possibility of extending the computer program even further, to enable it, in particular, to accommodate computer configurations involving more than two modes of operation.

TABLE OF CONTENTS

FIGURES

TABLES

LIST OF SYMBOLS*

i,j,k,ℓ,m	Non-negative integers - indicies of summation.
i',j',k'	Biased summation indicies; e.g. $i' = i + c$ with c a constant.
ℓ	Integer (subscript) indicating mode of operation.
x	Integer (subscript) indicating computer stage (e.g. CPU, I/O unit, memory module, etc.)
$Q_{x,\ell}$	Number of identical operational units needed at stage x in mode ℓ.
r	$Q_{x,1} - Q_{x,2} - 1$ if units that were active in mode 1 but are initially not needed in mode 2 can be treated as spares; $r = 0$ otherwise (or if $Q_{x,2} \geq Q_{x,1}$).
S_x	The number of spare units initially available to stage x.
t,τ,τ'	Time variables
$\tau_{x,\ell,s}$	Time needed to test a spare at stage x during mode ℓ.
λ_x	Hazard rate for an active unit at stage x.
μ_x	Hazard rate for a dormant unit at stage x.
K_x	λ_x/μ_x = dormancy factor for stage x.
λ_i	Rate of occurrence of "category i" failures; i.e. failures that prevent the system from operating in mode ℓ for any $\ell < i$, $i = 2,3,\ldots$, but do not preclude operation in any mode $\ell \geq i$.
γ_x	Rate of occurrence of transient failures at stage x.
$C_{x,\ell}^{(i,t)}$	The probability that exactly i of the S_x spares available at stage x have been used after t time units of operation in mode ℓ.

*The subscripts on these symbols are appended only when it is necessary to distinguish explicitly between the various modes, stages etc. Thus, for example, the symbol $Q_{\ell x}$ is frequently represented by simply Q with the subscripts implied.

$R(t)$ — System reliability; i.e. the probability that the system is still operating successfully at time t.

$R_\ell(t)$ — Probability that the system is still operating at time t and that it is operating in mode ℓ.

$R_{x,\ell}(S_x, t)$ — The probability that stage x has operated successfully in mode ℓ for t time units, given that S_x operational spares were initially available.

$H_x(\tau)$ — Transition probability density; i.e. probability density of a failure in stage x resulting in a successful degeneration to mode 2 due to the lack of any remaining spares.

$S_x(t, \tau)$ — Probability that stage x survives until time τ in mode 1 and from time τ to time t in mode 2.

$T_d(t)$ — Probability that system successfully enters mode 2 due to a deficit of spares in some stage and (given no category three failures) survives in that mode until time t.

$T_2(t)$ — Probability that system successfully enters mode 2 following a category two failure and (given no category three failures) survives in that mode until time t.

$C_{x,\ell,i,j,k}$ — The conditional probability that the system can recover from a fault in stage x during mode ℓ, given that the fault belongs to fault class j, is detected by detector i, and that the k^{th} spare for stage x is the first spare found to be operational.

$d_{x,\ell,j}$ — Fraction of faults at stage x belonging to class j during mode ℓ.

$C_{x,\ell,k}$ — Coverage (i.e. the conditional recovery probability) for stage x during mode ℓ given that the k^{th} spare is the first spare found to be operational;

$$C_{x,\ell,k} = \sum_{i,j} d_{x,\ell,j} \; C_{x,\ell,i,j,k}$$

$C_{x,\ell}$ — $C_{x,\ell,1}$

$\delta_{x,\ell}$ — $C_{x,\ell,1}/C_{x,\ell,2}$

$C'_{x,\ell,k}$, $\delta'_{x,\ell,k}$ — The superscript (') on these terms indicates transitional coverage parameters: i.e. $C'_{x,\ell,k}$ denotes the coverage in stage x during mode ℓ when none of the k-1 remaining spares are operational and it is hence necessary to degenerate to mode $\ell + 1$.

$P_{x,\ell,i,j}$ — The probability that a class j fault in stage x during mode ℓ would be detected by detector i were it the only detector operating.

$P_{x,\ell,i,j}\, f_{x,\ell,i,j}(t)$ — Rate at which detector i would detect category j faults in stage x during mode ℓ were it the only detector operating ($\int f_{x,\ell,i,j}(t)\, dt \triangleq 1$).

$F_{x,\ell,i,j}(\eta) \int_0^{\eta} f_{x,\ell,i,j}(t)\, dt$

$P_{x,\ell,i,j}\, g_{x,\ell,i,j}(t)$ — Rate at which detector i detects category j faults in stage x during mode ℓ given that all other relevant detectors are also in operation.

$P'_{x,\ell,i,j}$ — Probability that a category j fault in stage x detected by detector i during mode ℓ is successfully isolated to the faulty unit.

$P'_{x,\ell,i,j}\, h_{x,\ell,i,j}(t)$ — Isolation rate associated with detector i following a category j fault in stage x during mode ℓ $\left(\int h_{x,\ell,i,j}(t)\, dt = 1\right)$.

$P''_{x,\ell}$ — Probability that a spare can be successfully tested in stage x during mode ℓ.

$r_{x,\ell,i,j}(\tau, \tau') = r'_{x,\ell,i,j}(\tau)\, r''_{x,\ell,i,j}(\tau, \tau')$ — Probability of successful recovery in stage x during mode ℓ following a class j fault detected by detector i when the detection and isolation rates are τ and τ', respectively.

INTRODUCTION

The reliability model implemented in CARE II (i.e., the Raytheon extension to the CARE program) can be described with reference to Figure 1. The computer system being modeled is assumed segregated into n stages ($1 \leq n \leq 8$) with switchable spares separately provided for each stage. Two modes of operation are possible. In mode 1, Q_{1i} identical units must be functioning at stage i, i = 1,2,..., n , for the system as a whole to be operational in that mode; in mode 2, Q_{2i} units are required at stage i.

The system begins operation in mode 1 (cf. Figure 1) and continues in that mode until a failure occurs that either forces the system into mode 2 or else causes a system failure. The latter can be caused by a coverage failure or by a category three hardware failure. This latter term includes all those failures that, by themselves, preclude further operation regardless of the number of functioning units at any stage. (Category three failures are frequently referred to as single-point failures.)

Degeneration to mode 2 can be caused either by a category two hardware failure or by spares exhaustion in any particular stage; i.e. by a failure in any one of the Q_{1i} units needed at stage i after all of the available spares for that stage have already been used. A category two failure is one that prevents further operation in mode 1 even though a sufficient number of units is available at each stage. (E.g., if mode 1 operation entails the comparison of the outputs generated by two independent, parallel systems, a failure in the comparator could constitute a category two failure.)

Similarly, the system will continue to operate in mode 2 until a coverage failure, a category three failure, or a failure following the depletion of all

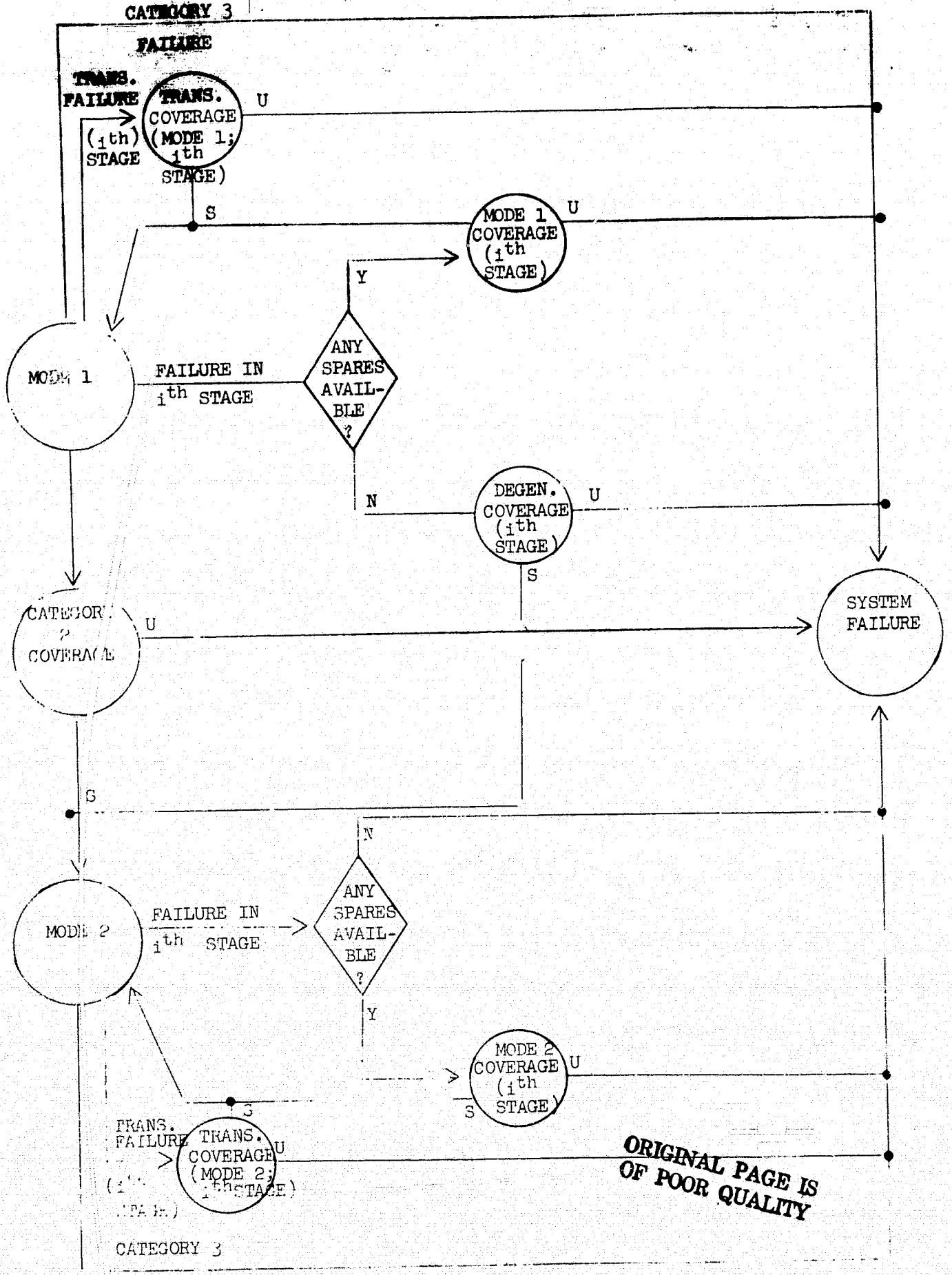


FIGURE 1
CARE II RELIABILITY MODEL

spares available for the stage in question causes the whole system to fail.

It will be noted from Figure 1 that both permanent and transient hardware failures are modeled. Since transient failures by definition do not permanently disable any hardware, there are only two possible outcomes of such a failure: either the system recovers from a transient failure and successfully resumes the application programs or it does not. The latter case is defined as a system failure.

The fidelity with which this model determines the reliability of an actual system is highly dependent upon the accuracy with which the various coverage probabilities indicated in Figure 1 can be determined. That is, given a hardware failure of a particular sort, and the availability of the necessary spares, what is the conditional probability that computer system can actually recover and resume its intended function? Because of the importance of these parameters, a coverage model was also postulated and programmed as part of the CARE II package. This model provides a means for calculating coverage as a function of the type of failure experienced, its temporal characteristics (i.e., permanent or transient), the number of spares that must be tested before an operational one is found, the time delays associated with the various fault detection and isolation mechanisms, and the probability that a successful recovery can be achieved given that t_d seconds were needed to detect the failure and t_i seconds needed to isolate it.

Details of the coverage model implemented in CARE II are presented in Section III. The next section (Section II), however, first describes the CARE II reliability model itself. Some specific simple coverages and reliability problems are solved analytically in Section IV in an effort to illustrate

the generality and flexibility of the CARE II model. Finally, Section V concludes with a discussion of potential further extensions of the presently implemented reliability model, including the possibility of expanding it to include systems capable of operating in three or more modes.

II. Reliability Model Derivation

The CARE II reliability model is based on the assumption that each component comprising the computer system exhibits a constant failure or hazard rate λ . This assumption, which is almost universally made in deriving computer reliability models, is well supported by experimental evidence. The two major limitations to its validity are due to the "infant mortality" phenomenon resulting in a decreasing failure rate for new, untested parts and to wear-out mechanisms (e.g. tungsten evaporation in a incandescent light-bulb filament) causing the failure rate to increase with age. Since the infant mortality phenomenon can be (and, in those cases in which reliability is of concern, presumably would be) eliminated by appropriate screen-and-burn-in procedures,and since wear-out mechanisms are virtually nonexistant in solid-state devices, the constant failure-rate assumption appears to be entirely adequate for the present purpose.

If $P(t)$ denotes the fraction of elements of a particular class operating at time t, then $-P'(t)dt$, with $P'(t)$ denoting the time derivative of $P(t)$, indicates the fraction of elements failing in the time interval $(t, t+dt)$. The failure rate associated with this class of elements is then:

$$\lambda(t) = - \frac{P'(t)}{P(t)} \qquad (1)$$

(i.e. the fraction of presently operating elements failing per unit time). If $\lambda(t) = \lambda$ is constant, then the solution to equation 1 (subject to the boundry condition that $P(0) = 1$) is:

$$P(t) = e^{-\lambda t}$$

Further, if an irredundant computer unit is composed of n_i elements having failure rate λ_i, $i = 1,2,\ldots,N$, then the probability that that unit is still operating at time t, given that it was operating at time zero, is the probability

that all of its component parts are operating at time t; i.e.

$$P(t) = \prod_{i=1}^{N} (e^{-\lambda_i t})^{n_i} = e^{-(\sum_{i=1}^{N} n_i \lambda_i)t} = e^{-\lambda t} \qquad (2)$$

with $\lambda = \sum_{i=1}^{N} n_i \lambda_i$ simply the sum of the failure rates of the unit's component parts.

Now, if Q of these units are needed for a given computer configuration to function properly and if i standby spares are provided which can be switched in to replace any defective units, the probability that exactly i such spares have been required by time t is simply the probability that exactly i units out of a total of Q + i -1 units in the configuration have failed and that the $(Q + i)^{th}$ unit is still functioning. To see this, assign the units used up to time t consecutive numbers from 1 to Q + i, with units 1 through Q representing the original Q operating units, unit Q + 1 the first spare switched in to replace a defective unit, unit Q + 2 the second spare switched in, etc. Exactly i spare units will have been used by time t if and only if exactly i of the units bearing the numbers 1,2,3,..., Q +i -1 have failed. Note that the $(Q + i)^{th}$ unit must still be operational since, were it not, at least i + 1 spares would have been required. But the probability P(i,n) of exactly i failures in n chances, when the probability of an individual failure is q = 1 - p is given by the well-known binominal distribution:

$$P(i, n) = \binom{n}{i} q^i p^{n-i}$$

Consequently, the probability $G(i,t)$ that i of Q + i-1 units have failed by time t and that the $(Q + i)^{th}$ unit is still functioning is $P(i , Q + i -1)$ with $e^{-\lambda t}$ the probability that any one of them has survived until time t; i.e.:

$$G(i,t) = \binom{Q+i-1}{i}\left(1 - e^{-\lambda t}\right)^{i}\left(e^{-\lambda t}\right)^{Q} \qquad (3)$$

Note that this last conclusion implicitly assumes equal failure rates for all Q + i units. If, however, the units that are operational but are not currently being used are placed in a dormant mode until they are needed (e.g. the units are not powered until they are actually needed), this assumption of identical failure rates may not be valid; the dormant units may well fail at a rate μ significantly less than the active unit failure rate λ . This added degree of freedom potentially complicates the expression for the probability that exactly i units are required since the probability that a particular unit is still operational is now a function of when it was placed in the active mode which in turn, is determined by the number of prior failures.

It can be shown*, however, that the probability of using exactly i spares when Q active units are needed and the active and standby unit failure rates are λ and μ respectively, is equal to the probability of using exactly i spares when $\lambda Q/\mu$ active units are needed for successful operation and the failure rate is μ for both active and standby units.

*J.J. Stiffler, On the Efficacy of R-On-M Redundancy, IEEE Trans. on Reliability, April 1974.

That is, from equation (3),

$$G(i,t) = \binom{KQ + i - 1}{i} \left(1 - e^{-\mu t}\right)^{i} \left(e^{-\mu t}\right)^{KQ} \qquad (4)$$

with $K = \lambda/\mu$. This observation considerably simplifies the subsequent derivations.

Note that $KQ + i - 1$ need not be an integer here. The binomial coefficient:

$$\binom{KQ + i - 1}{i} = \frac{(KQ + i - 1)(KQ + i - 2) \ldots (KQ)}{i!}$$

is still defined for noninteger values of $KQ + i - 1$ and equation (4) still holds.

An additional complication results when the possibility of a coverage failure is acknowledged since the possibility then exists that the system was unable to recover even though a spare was available. Moreover, the probability of successful recovery may well be further diminished when one or more of the spares has already failed by the time it is needed since this presumably increases the total time needed to recover. In the CARE II reliability model, the coverage probability (determined using the coverage equation: cf., Section III) is expressed in the form $C\delta^{(k - 1)}$, with k the number of spares that must be tested before an operational one is found. That is, if the first spare tested is operational, the probability of recovery is C; if the first spare has failed but the second is functioning, the recovery probability is diminished by the

factor δ; if two failed spares are encountered the recovery probability is decreased by the factor δ^2; etc.

Fortunately, the effect of imperfect coverage can be included in equation (4) simply by replacing the product KQ by the parameter $M = KC\delta^{-1}Q$ and by multiplying the result by δ^i. The resulting probability thus becomes

$$G(i,t) = \binom{M+i-1}{i} \delta^i (1-e^{-\mu t})^i e^{-KQ\mu t} \qquad (5)$$

A proof of the validity of this result is presented in the appendix to this report.

Equation (5) represents the probability that the Q-unit ensemble in question survives until time t given exactly i hard (permanent) failures. The CARE II model also includes the possibility of transient failures. The coverage model (cf. Section III) provides a means of determining the probability P_r of recovering from a transient as well as from a permanent failure. If transient failures occur at the rate γ' failures per unit time, nonrecoverable failures then occur at the rate $\gamma = (1-P_r)\gamma'$. The probability G(i,t) in equation (5) must, therefore, be multiplied by the probability $e^{-\gamma t}$ that no nonrecoverable transients occur by time t in order to obtain the probability that the Q-unit ensemble survivesuntil time t using i spares when both hard and transient failures are taken into account. The resulting expression thus becomes:

$$G(i,t) = e^{-\gamma t} \binom{M+i-1}{i} \delta^i (1-e^{-\mu t})^i e^{-KQ\mu t} \qquad (6)$$

With these preliminaries, we can now determine the reliability R(t) of the dual-mode computer system. First, let:

$$R(t) = R_1(t) + R_2(t) \qquad (7)$$

$R_1(t)$ denoting the probability that the system survives until time t in mode 1 and $R_2(t)$ the probability that it survives in mode 2. (That is, $R_2(t)$ is the probability that the system is still operating at time t but that it had to switch to mode 2 sometime prior to time t.)

Let $R_{x,\ell}(S_x,t)$ be defined by the expression:

$$R_{x,\ell}(S_x,t) = \sum_{i=0}^{S_x} G_{x,\ell}(i,t)$$

with $G_{x,\ell}(i,t)$ as defined in equation (6). (The subscripts ℓ and x here denote, respectively, mode ℓ and stage x, and S_x indicates the number of spares available at stage x.) Thus, $R_{x,\ell}(S_x,t)$ is the probability that stage x is able to survive in mode ℓ until time t using no more than the S_x spares provided for it. The expression for $R_1(t)$ is then:

$$R_1(t) = \prod_x R_{x,1}(S_x,t) \cdot e^{-\lambda_2 t} \; e^{-\lambda_3 t} \qquad (8)$$

The product over x in equation (8) thus represents the probability that all stages have survived in mode 1 with none requiring more than its allotted number of spares. The two exponentials in equation (8) are simply the probabilities of no category two and no category theee failures, respectively.

In order to determine $R_2(t)$ it is convenient to define some additional terms. First, note that:

$$P_2(t) = (T_{2,1}(t) + T_{2,2}(t)) \; e^{-\lambda_2 t} \qquad (9)$$

where $P_2(t)$ the probability that the computer system successfully enters mode 2 following a category 2 failure and survives in mode 2 until time t, $T_{2,1}(t)$ the probability that it successfully enters mode 2 due to a spares deficit in some stage and survives in mode 2 until time t, $e^{-\lambda_2 t}$ the probability of no [illegible] (single-point) failures.

Now let $H_x(\tau)$ be the transition probability density for stage x; i.e., the probability density of a failure in stage x resulting in a successful degeneration to mode 2 due to the absence of any remaining operational spares. It follows that:

$$H_x(\tau) = \left[Q_{x1} \lambda_x \right] \sum_{i=0}^{S_x} \left[G_{x1}(S_x - i, \tau) \right] \left[(1 - e^{-\mu_x \tau})^i \right] \left[C'_x (\delta'_x)^i \right] \qquad (10)$$

The first bracketed factor is simply the rate at which failures afflict the Q_{x1}-unit ensemble defining stage x in mode 1. The second factor represents the probability that all but i of the S_x spares for stage x have been used by time τ and that stage x is still operational at that time. The third factor is the probability that the i remaining spares have all failed by time τ. The last term is the recovery probability given that i spares must be tested and that degeneration to mode 2 is necessary. (The "primes" on the C δ terms indicate that the transitional coverage may be different than the coverage when no change is needed even though the same number of spares must be tested in both cases. The coverage model described in Section III provides a means for determining this difference by allowing user to specify transitional parameter.) The product of these terms, summed over all i ($i = 0,1, \ldots, S_x$) is the desired probability density.

Further, let $S_x(t,\tau)$ be the probability that stage x survives until time τ in mode 1 and from time τ to time t in mode 2. This probability can be expressed in the form:

$$S_x(t,\tau) = \sum_{\ell=0}^{S_x} \sum_{j=0}^{S_x - \ell} \left[G_{x1}(\ell, \tau) \right] \left[\binom{S_x}{j} (1 - e^{-\mu_x \tau})^{S_x - \ell - j} e^{-j\mu_x \tau} \right] \left[R_{x,2}(j', t - \tau) \right] \qquad (11)$$

The bracketed factors denote, respectively, the probability that stage x survives until time τ in mode 1 using exactly ℓ spares, the probability that

exactly j of the remaining S_x-ℓ spares are still operational at time τ, and the probability that stage x survives for the remaining $t - \tau$ in mode 2 given that j spares were operational at time τ (cf. equation 8). The definition of the parameter j' depends upon whether or not the Q_{x1}-Q_{x2} active units that were needed in mode 1 but are not required in mode 2 are reassigned to the spares pool. If they are, $j' = j + Q_{x1} - Q_{x2}$; if they are not $j' = j$. The product of these terms summed over all combinations of unused and functioning spares yields the desired probability.*

---

*This expression for $S_x(t,\tau)$ assumes that all remaining spares are tested immediately following degeneration to mode 2. This allows any defective spares to be discarded at that time and hence, if $\delta_{x2} < 1$, decreases the probability of a coverage failure in mode 2. If this is not done $S_x(t,\tau)$ becomes:

$$S_x(t,\tau) = \sum_{\ell=0}^{S_x} \sum_{i=0}^{S_x' - S_x} G_{x,2}(i,\ t-\tau)\ G_{x,1}(\ell,\ \tau)$$

$$+ \sum_{\ell=0}^{S_x} \sum_{j=\Delta+1}^{S_x' - \ell} \sum_{i=\Delta+1}^{j} G_{x,1}(\ell,\tau) \binom{j-\Delta-1}{i-\Delta-1} \delta^{j-i} (1-e^{-\mu_x \tau})^{j-i}\ e^{-(i-\Delta)\mu_x \tau} G_{x,2}(i,t-\tau)$$

with

$$\Delta = S_x' - S_x = \begin{cases} 0 & \text{Excess active units not used in Mode 2.} \\ Q_{x1} - Q_{x2} & \text{Excess active units used as spares.} \end{cases}$$

This expression assumes that the reassigned active units are the first to be used in the event of subsequent failures.

We can now express $T_2(t)$ and $T_d(t)$ in terms of previously defined quantities:

$$T_d(t) = \sum_x \int_0^t \left[\prod_{y \neq x} S_y(t,\tau)\right]\left[H_x(\tau)\right]\left[R_{x,2}(\tau, t-\tau)\right]\left[e^{-\lambda_2 \tau}\right] d\tau \qquad (12)$$

$$T_2(t) = \int_0^t \left[\prod_y S_y(t,\tau)\right]\left[\lambda_2 C_2 e^{-\lambda_2 \tau}\right] d\tau$$

The first bracketed factor in the expression for $T_d(t)$ is the probability that each of the stages comprising the computer system except stage x survives in mode 1 until time τ and in mode 2 from time τ to time t (cf. equation (11)). The second factor is the probability density of a degeneration from mode 1 to mode 2 at time τ caused by a spares deficit in stage x (see equation 10). The third factor is the probability that stage x then survives in mode 2 from time τ to time t given a total of r functioning spares at time τ. The definition of the parameter r, like that of parameter j' in equation 11, depends on whether the $Q_{x1} - Q_{x2}{}^{-1}$ former active and still operational units not needed in mode 2 are reassigned as spares. If they are $r = Q_{x1} - Q_{x2}{}^{-1}$; if they are not, r = 0. The last factor in the expression for $T_d(t)$ is just the probability that no category two failures occur before the degeneration to mode 2; after that time, of course, category two failures are irrelevant. The product of these factors then is the probability density that the system as a whole survives to time τ in mode 1 and then continues successfully in mode 2 until time t. Since the degeneration can occur at any time τ in the range (0,t), this product, integrated over this entire interval, provides the desired probability $T_d(t)$.

The expression for $T_2(t)$ differs from that for $T_d(t)$ in that the cause of the degeneration is now a category two failure; consequently the product $H_x(\tau)\, R_{x,2}(\tau, t-\tau)$, representing the probability density of a degenerative failure at stage x at time τ followed by its successful operation in mode 2 until time t, is replaced by $\lambda_2 C_2 e^{-\lambda_2 \tau}$, the probability density of a recoverable category two failure at time τ. The product in the expression for $T_2(t)$ is now over all stages, since in this case, none of them is the cause of the degeneration. That is, for successful operation through a category two failure, all stages must operate successfully in mode 1 prior to, and in mode 2 following, this event.

The reliability model implemented in CARE II thus determines the reliability R(t) defined in equation 7 using the intermediate quantities defined in equations 8 and 9 through 12. As can be seen, it is a highly versatile model, allowing arbitrary active and dormant failure rates to be specified for each of up to eight stages with arbitrary numbers of spares assigned to each stage. Furthermore, the concept of coverage is fully integrated into the model with provision for specifying recovery probability as a function of the stage in question, the number of spares that have to be tested and the mode of operation (mode 1, mode 2, or transitional). Unfortunately the CARE II user can rarely, if ever, be expected to be able to assign these coverage terms with any degree of confidence. For this reason, a coverage model was also defined and implemented as part of CARE II. This model, described in the next section, provides a means of determining these coverage parameters in terms of more basic parameters which are presumably more readily supplied, or at least more readily estimated, by the user.

III. Coverage Model Derivation

The purpose of the coverage model is to determine the coverage coefficients associated with the computer system as a function of the stage afflicted by the failure, the operating mode (mode 1, mode 2, or transitional), the type of fault (permanent or transient), and the number of failed spares encountered in the search for a functioning one. Although the coverage model implemented in CARE II can be used to evaluate the coefficient C_k, (the coverage given k - 1 failed spares) for any k, the use of such information would result in a somewhat more complicated reliability model than that described in the previous section. There it was assumed that C_k was of the form $C_k = C\delta^{(k-1)}$ for all i = 1,2,.... The coverage model is therefore used to determine C_1 and C_2 only, with δ defined as the ratio C_2/C_1. Since $C\delta^{(k-1)}$ is presumably a reasonably good approximation to C_k for small k (and is exact for k = 1 and 2 when $\delta = C_2/C_1$) and since the likelihood of several consecutive failed spares is generally small in any event, the increased computational time that would be needed to use the more general coverage coefficients C_k was not felt to be justified.

Conceptually, coverage can be broken down into three basic components: fault detection, fault isolation, and applications program recovery. Any one of the following events constitutes a coverage failure: the failure to detect the fault, the failure to isolate it to the affected unit and to replace that unit with a functioning spare, or the inability to effect a timely recovery of the applications program. The mechanism by which the failure is detected presumably determines the isolation and recovery procedures; i.e., there is direct linkage, called a DIR mechanism, from a detection to an isolation [illegible] a recovery proced[illegible]

between a particular fault and a particular detector, however, may be more complex. Frequently, several different detectors may be capable of detecting a certain fault. Which detector actually succeeds is a function of the computer operation being carried out when the fault becomes manifest. The CARE II coverage model provides a means of determining the probability that a fault in any specific class or subclass* is eventually detected by a given detector in competition with other detectors as well as the distribution of the time delay before this detection takes place. This information is then used in combination with user-provided statistics concerning the isolation and recovery mechanisms associated with that detector to determine a coverage coefficient for that detector. The summation of the probabilities of these mutually exclusive coverage events then establishes the coverage for the fault class in question.

The concept of a fault class is basic to the CARE II coverage model. It cannot be assumed, for example, that if detector A detects 90% of all faults in a given computer stage and detector B also defects 90% of these faults, that together they detect $1-(1-0.9)^2 = 99\%$ of all faults. It may well be that they both fail to detect the same 10% of the possible faults and hence that together they are no more effective than either is alone. In the CARE II coverage model, this difficulty was circumvented by requiring the user to categorize the possible faults afflicting any computer stage.

A fault class is defined as a group of faults whose possible detection by any specific detector is statistically independent of its possible detection [illegible]

*The term fault class is used to denote a category of faults afflicting a stage; a fault subclass refers to a category of faults pertaining to a substage. For purposes of this discussion this distinction is not important.

tectors compete against each other across fault classes; they compete statistically independently, however, within any specific class. In the previous example, the totality of possible faults at the stage in question, for instance, might be divided into four disjoint classes each representing 25% of the total. If detector A were then capable of detecting 100% of the faults in the first two classes and 80% of the faults in the third and fourth classes, and detector B capable of detecting 100% of the faults in classes 1, 2 and 3 and 60% of the class 4 faults, they both would be able individually to detect 90% of the faults as before. Together, however, they would detect:

$$3/4 + 1/4\ (1-(1 - 0.8)\ (1 - 0.6)) = 98\%$$

of the faults. If in contrast, both detectors were 100% effective in the first three classes and 60% effective in the fourth, so that again both are 90% effective overall, their combined effectiveness would be:

$$3/4 + 1/4\ (1 - (1 - 0.6)^2) = 96\%$$

The task of segregating faults into classes requires careful analysis of the possible faults that can occur and of the characteristics of the available detectors. The success with which this categorization has been accomplished can be tested by determining for each fault within a given class, its probability of detection by each of the available detectors.

If this set of detection probabilities is identical for all faults in any class, a sufficient number of classes has been defined; otherwise, further subdivision or reclassification is needed. Although fault classification does require detailed knowledge of the types of faults that can occur, no coverage model can provide a meaningful measure of coverage, unless this information or its equivalent is determined.

Once the faults relevant to each computer stage are categorized, the user must then characterize each detector i for each fault class j in each stage by a detection probability, a detection rate $f(t) = f_{ij}(t)$ (as usual, subscripts will be omitted in the following discussion unless they are needed for purposes of clarity), and a detection delay (for hardware detectors) or a scheduling rule (for software diagnostics). He must in addition associate with each detector an isolation procedure (characterized by an isolation probability and an isolation rate h(t), and a recovery procedure (characterized by the probability $r(\tau, \tau') = r'(\tau)\, r''(\tau + \tau')$ with τ and τ' the times needed for detection and isolation, respectively. (This form for $r(\tau, \tau')$, although somewhat restrictive, is felt to be sufficiently general to encompass the vast majority of recovery mechanisms. Factoring $r(\tau, \tau')$ in this way implies that the recovery probability is the product of two terms: (1) an error-propagation recovery probability which is a function only of the time τ during which the fault condition existed but was undetected; and (2) a time-lost recovery probability which is a function of the total time $\tau + \tau'$ elapsed between the occurrence of the error and its isolation. The reason for distinguishing between these two conditions is that during the error-propagation period, the effect of the still undetected error could propagate

to other computer elements, thereby complicating recovery and reducing the probability below that resulting from consideration of the total "down-time" $\tau + \tau'$ alone.

On the basis of this user-supplied information, the coverage model determines the resulting coverage C_{ijk}, (when k spares have to be tested) for each fault class j, and detector i, and, for each stage, calculates the coverage:

$$C_k = \sum_j d_j \sum_i C_{ijk} \qquad (13)$$

with d_j the fraction of total faults belonging to class j. That is, C_{ijk} represents the fault class j coverage associated with the DIR mechanism i. Since detection by detector i precludes detection by any other detector, the summation over i of these terms represents the total coverage for fault class j and the weighted sum over all fault classes thus determines the overall coverage for the stage in question.

Let P_{ij} and P'_{ij} be, respectively, the detection and isolation probabilities associated with detector i operating alone in the presence of a class j fault. Let P''_j be the probability of successfully testing a spare required as a result of a class j fault and let τ_s represent the time needed to complete this test. Finally, let $P_{ij}\, g_{ij}(t)$ be the probability density of the detection of a fault in class j by detector i when the total fault detector environment is taken into account. (Thus, $f_{ij}(t)$ is the detection rate of the detector i when no competing detectors are present; $g_{ij}(t)$ the analogous function when these competing detectors are

considered.) It will be shown presently that $g_{ij}(t)$ can be expressed in terms of the set of density functions:

$$P_{\ell j}\, f_{\ell j}\,(t), \quad \ell = 1, 2, \ldots, i, \ldots$$

The coverage term C_{ijk} can be expressed in terms of the functions and parameters defined in the preceding paragraphs in the form:

$$C_{ijk} = P_{ij}\, P'_{ij}\, (P''_j)^k \int_0^\infty g_{ij}(\tau)\, r'_{ij}(\tau) \int_0^\infty h_{ij}(\tau' - k\tau_s)\, r''_{ij}(\tau+\tau')\, d\tau' d\tau \qquad (14)$$

The detection probability density function for the i^{th} detector is $P_{ij}g_{ij}(\tau)$ and the associated isolation density function is, by definition, $P'_{ij}h_{ij}(\tau')$. If k spares must be checked in order to recover successfully from a fault, the overall recovery probability is decreased by the factor $(P'')^k$, with P'' the probability of successfully checking out a spare, and the isolation delay is effectively increased by the factor $k\tau_s$. The term C_{ijk} is thus equal to the conditional probability that the system can still recover given a τ-second detection delay times the detection probability density function, multiplied by the conditional probability that the system can recover given that it has survived a τ-second detection delay and must in addition undergo a total of $\tau + \tau'$ seconds down-time, times the corresponding isolation density function, the whole thing integrated over all τ and τ'', and multiplied by $(P'')^k$.

The only term in equation (14) not immediately attainable from the information provided by the user is the conditional density function $g_{ij}(\tau)$.

for this term is a function, not just of the detector i, but of the entire ensemble of detectors and their interrelationships. (Note that the same competitive relation does not exist between isolation and recovery procedures since these procedures are uniquely determined by the outcome of the competition among the detectors.) In order to define $g_{ij}(\tau)$, it will be useful to introduce some new terminology. (For notational convenience, the subscript j denoting the fault class in question will be dropped in the ensuing discussion.) Let $T_i = n_i T$ be the periodicity with which software diagnostic program i is scheduled, let n_c be the least common multiple of the n_i, and let $n_c T$ be defined as the major cycle. Let t_i, $t_i + \Delta t_i$ be the start and finish times for detector or diagnostic program i measured with respect to the occurrence of a fault for hardware detectors, and relative to the start of a major cycle for software diagnostics.

Let $t_j^{\ell} = t_j \ell\,(i)$ be the maximum value (with respect to ν) not exceeding $t_i + T_i$ of the expression $(t_j + \nu T_j - (\ell - 1)T_i)$; that is, let $t_j^{\ell} + (\ell - 1)\,T_i$ be the time of the last occurrence of diagnostic program j in the interval separating the $(\ell - 1)^{st}$ and the ℓ^{th} occurrence of diagnostic program i. Finally let:

$$F_i(\eta) = \begin{cases} 0 & \eta < 0 \\ \int_0^{\eta} f_i(\alpha)\, d\alpha & 0 < \eta < \Delta t_i \\ 1 & \eta > \Delta t_i \end{cases}$$

and let $\bar{F}_i(\eta) = 1 - F_i(\eta)$. (Note that $f_i(t)$ is a normalized detection probability density; its integral over the Δt_i - second detection interval is unity. Note, too, that the detection delay t_i is treated here as an explicit parameter. Thus the detection probability density associated with the i^{th} detector is of the form $P_i f(t - t_i)$ with f(t) nonzero only over the interval $0 \le t \le \Delta t_i$.)

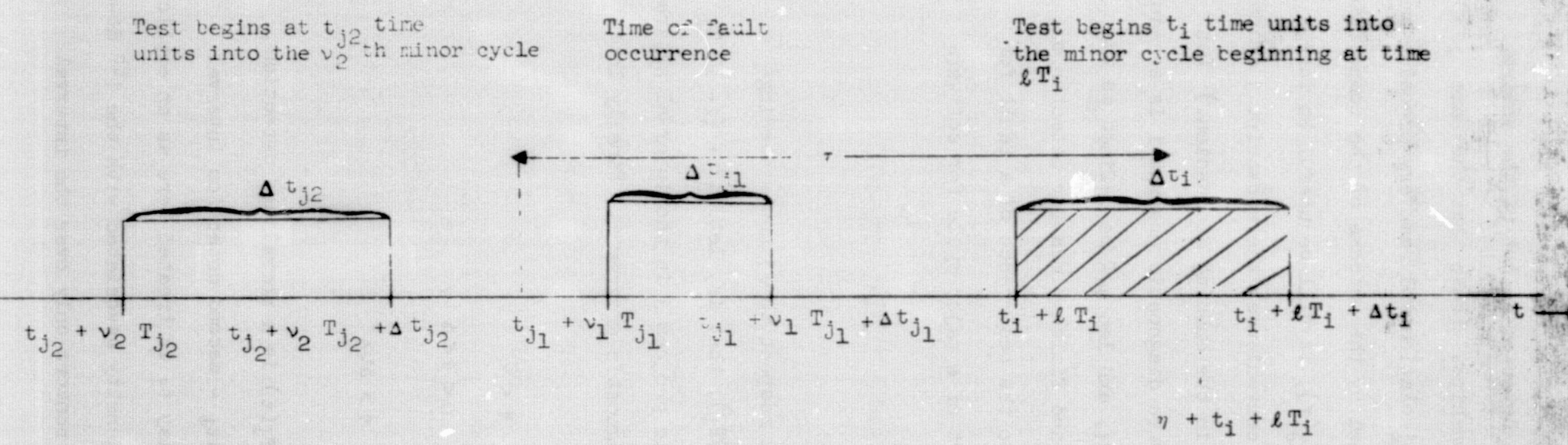


FIGURE 2

SOFTWARE DIAGNOSTIC SCHEDULING

We next observe that the detection rate of the i^{th} software diagnostic program when competing only with the other diagnostic programs is for,

$0 \leq \eta \leq n_i T$,

$$g_i'(\tau) = \frac{1}{n_c T} \sum_{\ell=1}^{n_c/n_i} \int_0^{\Delta t_i} \prod_{j \neq i} \left[1 - P_j \, \overline{F}_j(\eta - \tau + n_i T + t_i - t_j^{\ell}) \right] f_i(\eta) \, d\eta \qquad (15)$$

and is identically zero elsewhere. The product here is taken over all j representing other software diagnostic programs. This expression is most easily explained with reference to Figure 2. The crossed-hatched rectangle there indicates the time interval during which the i^{th} diagnostic routine is run for the $(\ell + 1)$st time during a major cycle. If this routine is to detect a fault which occurred exactly τ seconds earlier, all other diagnositc programs which were run between these two instances of time (shown as dashed lines in Figure 2) must have failed to detect the fault. The probability of this event is given by the product over j in equation (15). (It is assumed here that if a fault occurs while the j^{th} routine is being run, the probability that that fault is detected before the routine is concluded is $P_j \int_t^{\Delta t_j} f_j(\tau) \, d\tau = P_j \overline{F}(t)$, with t the time the fault occurred relative to the beginning of the routine in question.) This product multiplied by the detection rate $f_i(\eta)$ of the i^{th} diagnostic routine and integrated over all η yields the conditional detection rate of the i^{th} software diagnostic test during its $(\ell + 1)$st execution in a major cycle. It remains only to sum this expression over all runs in each major cycle to obtain the desired detection rate.

The condition detection rates for software detectors when competing with both hardware and other software detectors can then be expressed in the form:

$$g_{ij}(\tau) = \prod_k \left[1 - P_k F_k(\tau - t_k)\right] g'_{ij}(\tau) \qquad (16)$$

with the product taken over all k corresponding to competing hardware detectors. That is, $g_{ij}(\tau)$ is simply equal to $g'_{ij}(\tau)$ times the probability that none of the competing hardware detectors has detected the fault first.

Similarly, the conditional detection rate of the i^{th} hardware detector in the presence of its competitive hardware and software detectors is:

$$g_{ij}(\tau) = \prod_{k \neq i} \left[1 - P_k F_k(\tau - t_k)\right] \left[1 - \sum_{j'} P_{j'} \int_0^\tau g'_{j'}(\eta)\, d\eta\right] f_i(\tau - t_i) \qquad (17)$$

The product here, taken over all k representing competitive hardware detectors, is again the probability that none of these detectors has already succeeded in detecting the fault. The second bracketed term multiplies this probability by the probability that none of the software detectors has been successful either. (The summation is over all j' competing software detectors. Note that the $g'_{ij}(\eta)$ functions represent mutually exclusive events; hence their weighted sum is indeed the probability density function of interest.)

These expressions for $g_{ij}(\tau)$ (equations 16 and 17) are used in equation (14) to determine the coverage terms C_{ijk} for all i, j, and k. These terms are used in equation (13) to calculate a coverage probability, for each stage and fault type, as a function of the number of spares that have to be tested.

The resulting coverage probabilities are then used in the reliability calculations described in Section II. The examples presented in the following section are intended to illustrate this procedure more fully.

IV. Some Examples

We first consider two examples involving the reliability model presented in Section II. Both examples are sufficiently simple that they can be solved analytically; each is intended to illustrate the significance of a subset of the various parameters defining the model.

In the first example we postulate a computer system consisting of only one stage with s spares. Also, in order to concentrate on the parameters of greatest interest, we assume that the category two and category three failure rates, λ_2 and λ_3, and the rate of occurrence γ of nonrecoverable transient failures are all negligible.

We then have, from equation 5,

$$G(i,t) = \binom{M + i - 1}{i} (i - e^{-\mu t})^i \delta^i e^{-KQ\mu t}$$

with $M = KCQ\delta^{-1}$.

If we further assume that $C = 1$ and that $\delta' = \delta$, conditions which generally hold at least approximately, we have, from equation 10,

$$H(\tau) = Q_1 \lambda C \sum_{i=0}^{S} \binom{M_1 + S - i - 1}{S - i} (i - e^{-\mu\tau})^S \delta^S e^{-KQ_1\mu\tau}$$

$$= Q_1 \lambda C \binom{M_1 + S}{S} (i - e^{-\mu\tau})^S \delta^S e^{-KQ_1\mu\tau}$$

and from equation 8,

$$R_1(t) = \sum_{i=0}^{S} \binom{M_1 + i - 1}{i} (1 - e^{-\mu t})^i \delta^i e^{-KQ_1 \mu t}$$

and,

$$R_{x,2}(r, t - \tau) = \sum_{i=0}^{r} \binom{M_2 + i - 1}{i} (i - e^{-\mu(t - \tau)})^i \delta^i e^{-KQ_2 \mu (t - \tau)}$$

On substituting the expression for $R_{x,2}(r, t - \tau)$ into equation 12, we obtain:

$$R_2(t) = m_a(t) = \int_0^t H(\tau) R_{x,2}(r, t - \tau) d\tau$$

$$- Q_1 \lambda C \binom{M_1 + S}{S} \sum_{i=0}^{r} \delta^{S+i} \binom{M_2 + i - 1}{i} \int_0^t (1 - e^{-\mu\tau})^S (1 - e^{-\mu(t - \tau)})^i e^{-K(Q_1 - Q_2)\mu\tau} d\tau e^{-KQ_2 \mu t}$$

Using the binomial expansion for $(i - e^{-\mu\tau})^S$ and $(i - e^{-\mu(t - \tau)})^i$, we can easily carry out the integration over τ, obtaining:

$$R_2(t) = Q_1 KC \binom{M_1 + S}{S} \sum_{i=0}^{r} \sum_{\alpha=0}^{S} \sum_{\beta=0}^{i} \delta^{S + i} \binom{M_2 + i - 1}{i} \binom{S}{\alpha} \binom{i}{\beta} \times$$

$$\times (-1)^{\alpha + \beta} e^{-\beta \mu t} \frac{1 - e^{-(\alpha - \beta + KQ_1 - KQ_2)\mu t}}{(\alpha - \beta + KQ_1 - KQ_2)} e^{-KQ_2 \mu t}$$

Since we will be interested in the limiting case in which the dormancy factor $K = \lambda/\mu \longrightarrow \infty$ (i.e. in which $\mu \longrightarrow 0$), we observe that $G(i,t)$ becomes, under these conditions,

$$\lim_{\substack{K \longrightarrow \infty \\ K\mu = \lambda}} G(i,t) = \frac{(QC\lambda t)^i}{i!} e^{-Q\lambda t}$$

(Note that in this event $G(i,t)$ is independent of δ. This is due to the fact that with $\mu = 0$ the first tested spare is guaranteed to be functioning.)

When $K \longrightarrow \infty$, $\mu \longrightarrow 0$ (with $K\mu = \lambda$) the above expressions thus become:

$$H(\tau) = Q_1 \lambda C \frac{(CQ_1 \lambda \tau)^S}{S!} e^{-Q_1 \lambda \tau}$$

$$R_{1,2}(r, t-\tau) = \sum_{i=0}^{r} \frac{(Q_2 C \lambda (t-\tau))}{i!} e^{-Q_2 \lambda (t-\tau)}$$

$$R_1(t) = \sum_{i=0}^{S} \frac{(Q_1 C \lambda t)^i}{i!} e^{-Q_1 \lambda t}$$

and

$$R_2(t) = \frac{(CQ_2\lambda)^{S+1}}{S!} \sum_{i=0}^{r} \frac{(Q_2 C\lambda)^i}{i!} \int_0^t \tau^S (t-\tau)^i e^{-(\quad)\lambda\tau} d\tau e^{-\quad\lambda\tau}$$

The integral in this last expression can be evaluated by again using the binomial expansion with the result that:

$$R_2(t) = \sum_{i=0}^{r} \sum_{\alpha=0}^{i} \frac{C^{S+i+1} Q_1^{S+1} Q_2^{i}}{(Q_1-Q_2)^{S+\alpha+1}} \binom{S+\alpha}{\alpha} \frac{(\lambda t)^{i-\alpha}(-1)^{\alpha}}{(i-\alpha)!} \left[1-e^{-(Q_1-Q_2)\lambda t} \sum_{\beta=0}^{S+\alpha} \frac{((Q_1-Q_2)\lambda t)^{\beta}}{\beta!}\right] e^{-Q_2\lambda t}$$

In either of these cases, of course, the total reliability is just $R_1(t) + R_2(t)$.

In order to reduce these results to a more tractable form, consider the special case in which $Q_1 = 3$, $Q_2 = 1$, $S = 2$. This corresponds to the situation in which the system begins operating in mode 1 with three active units and two spares. It switches to mode 2 after the third failure and operates using only one active unit. The remaining active unit that was still functioning in mode 1 and is no longer needed in mode 2 may be either discarded ($r = 0$) or reassigned to the spares pool and used in the event of a subsequent failure ($r = 1$). To emphasize the relative importance of the various parameters influencing the system reliability, we limit consideration to the following cases: $K = 1$ (dormant units are as likely to fail as active units) and $K = \infty$ (dormant units never fail); $\delta = 1$ (coverage is independent of the number of failed spares that have to be tested prior to recovery) and $\delta = 0$ (recovery is possible only if no spares have failed). The resulting expressions are tabulated in Table 1 as a function of $P = e^{-\lambda t}$, the probability that a single unit survives until time t, and the coverage C. Several of these expressions are then tabulated in Table 2 as a function of P for various values of C.

The preceding example considered the effect of various pertinent parameters (e.g. K,δ,C) on the reliability of a single-stage system. We now consider a

TABLE 1

SINGLE-STAGE RELIABILITIES

($n_1 = 3$, $n_2 = 1$, $S = $)

PARAMETERS	$R_1(\cdot)$	$R_2(\cdot)$
$K = 1$, $\delta = 1$ ($r = 0, 1$)	$\left[\frac{(1+3C)(2+3C)}{2} - 3C(2+3C)P + \frac{3C(1+3C)}{2}P^2\right]P^3$	$\frac{3C(1+3C)(2+3C)}{2}\left\{\left(\frac{1}{12} - \frac{P^2}{2} + 2/3\,P^3 - \frac{1}{4}P^4\right) + \frac{rC}{12}(1-P)^4\right\}P$
$K = 1$, $\delta = 0$ ($r = 0, 1$)	$\left[\left(1 + 3C + \frac{9}{2}C^2\right) - 3C\left(1+3C\right)P + \frac{9}{2}C^2P^2\right]P^3$	$\frac{(3C)^3}{8}\left\{\left(\frac{1}{12} - P^2/2 + 2/3\,P^3 - \frac{1}{4}P^4\right) + \frac{rC}{12}\left(1-P\right)^4\right\}P$
$K \to \infty$ ($r = 0, 1$)	$\left[1 + 3C\ln\left(\frac{1}{P}\right) + \frac{9}{2}C^2\ln^2\left(\frac{1}{P}\right)\right]P^3$	$\frac{27C^3}{8}\left[1 - P^2\left(1 + 2\ln\frac{1}{P} + 2\ln^2\frac{1}{P}\right)\right]P$ $+ \frac{r27C^4}{8}\left\{\left(\ln\frac{1}{P} - 3/2\right)\left[1 - P^2\left(1 + 2\ln\frac{1}{P} + 2\ln^2\frac{1}{P}\right)\right]P + \left(2\ln^3\frac{1}{P}\right)P^3\right\}$

TABLE 2

NUMERICAL RELIABILITIES

$(Q_1 = 3, Q_2 = 1, S = 2)$

PARAMETERS	UNIT RELIABILITY P	$R_1(t)$	$R_2(t)$ r = 0	$R_2(t)$ r = 1	TOTAL (r = 0)	TOTAL r = 1
C = 1	0.2	.0579	.4096	.6144	.4675	.6723
K = 1	0.4	.3174	.4752	.6048	.7926	.9222
δ = 1	0.6	.6826	.2688	.3072	.9514	.9898
	0.8	.9421	.0544	.0576	.9965	.9997
	0.9	.9914	.0083	.0085	.9997	.9999
C = .9	0.2	.0509	.3205	.4647	.3714	.5156
K = 1	0.4	.2828	.3719	.4632	.6547	.7460
δ = 1	0.6	.6219	.2103	.2373	.8322	.8592
	0.8	.8908	.0426	.0449	.9334	.9357
	0.9	.9622	.0065	.0066	.9687	.9688
C = 1	0.2	.0502	.1843	.2765	.2345	.3267
K = 1	0.4	.2829	.2138	.2721	.4967	.5550
δ = 0	0.6	.6307	.1210	.1383	.7517	.7690
	0.8	.9114	.0245	.0259	.9359	.9373
	0.9	.9805	.0037	.0038	.9842	.9843
C = 1	0.2	.1399	.4212	.5924	.5611	.8323
K → ∞	0.4	.4817	.3755	.4887	.8572	.9704
δ arbitrary	0.6	.8007	.1708	.1962	.9715	.9969
	0.8	.9695	.0287	.0304	.9982	.9999
	0.9	.9958	.0040	.0041	.9998	.9999

multi-stage system but with some of these parameters restricted in order to keep the analysis reasonably tractable. In particular, we assume that each of the n stages has the same failure rate λ, that $Q_{x1} = 2$, $Q_{x2} = 1$, $S_x = 1$, and $\mu_x = \lambda_x = \lambda$ for all stages. As before, we also assume that $\gamma = \lambda_2 = \lambda_3 = 0$.

Under the conditions just specified, equation 8 becomes

$$R_1(t) = P^{2n}\left[1 + 2C\ (1 - P)\right]^n$$

with $P = e^{-\lambda t}$ the reliability of a single stage in the n-stage system. It is also readily verified that equations 10, 11, and 8 become, respectively,

$$H_x(\tau) = 2\lambda C\ (2C + \delta)\ (1 - e^{-\lambda\tau})\ e^{-2\lambda\tau}$$

$$S_x\ (t,\tau) = a_o + a_1\ e^{-\lambda\tau} + a_2\ e^{-2\lambda\tau}$$

and

$$R_{x,2}\ (0,\ t - \tau) = P\ e^{+\lambda\tau}$$

with

$$a_o = r\ C\ P^2\left(\frac{C+\delta}{2}\ P - 1 - 2C\right)$$

$$a_1 = (1 + rC)\ (1 + 2C)\ P + C\ (r - \delta r - 1 - rC)\ P^2$$

$$a_2 = -C\ \left(1 + r - \frac{r\delta}{2} + \frac{3r}{2}\ C\right) P$$

As before, the parameter r = 1 if any unneeded units which were active in mode 1 and are still functioning are to be used as spares in mode 2 and r = 0

otherwise. (It is assumed that either r = 1 for all stages, or r = 0 for all stages.) Thus, from equation 12, since all stages have identical parameters,

$$R_2(t) = T_d(t) = \sum_x \int_o^t \prod_{y \neq x} S_x(t,\tau)\, H_x(\tau)\, R_{x2}(0, t-\tau)\, d\tau$$

$$= bnp\lambda \int_o^t (a_o + a_1 e^{-\lambda\tau} + a_2 e^{-2\lambda\tau})^{n-1} (e^{-\lambda\tau} - e^{-2\lambda\tau})\, d\tau$$

with $b = 2C(2C + \delta)$. Using the trinomial expansion

$$(a_o + a_1 x + a_2 x^2)^{n-1} = \sum_{\substack{i,j,k \\ i+j+k=n-1}} \frac{(n-1)!}{i!\, j!\, k!}\, a_o^i\, a_1^j\, a_2^k\, x^{j+2k}$$

and carrying out the integration, we obtain:

$$R_2(t) = bp \sum_{\substack{i,j,k \\ i+j+k=n-1}} \frac{n!}{i!\, j!\, k!}\, a_o^i\, a_1^j\, a_2^k \left[\frac{1 - P^{j+2k+1}}{j+2k+1} - \frac{1 - P^{j+2k+2}}{j+2k+2} \right]$$

When n = 2, for example, we find from the above that:

$$R(t) = R_1(t) + R_2(t)$$

$$= P^4 \left[1 + 2C(1 - P)\right]^2$$

$$+ \frac{C(2C + \delta)}{3} \left[(2 + 3C + d) - 2(C + 2d)\, P - 6(1 + 2C - d)\, P^2 \right.$$

$$\left. + 2(2 + 9C - 2d)\, P^3 - (7C - d)\, P^4 \right] P^2$$

with $d = (1 + 3C/2 + \delta/2)\, rC$

This result is tabulated in Table 3 as a function of P^2, the probability that a two-stage nonredundant system would have survived until time t, for various values of the parameters C, δ, and r.

TABLE 3

NUMERICAL RELIABILITIES

TWO-STAGE CONFIGURATION

$Q_2 = 1$, $Q_1 = 2$, S = 1

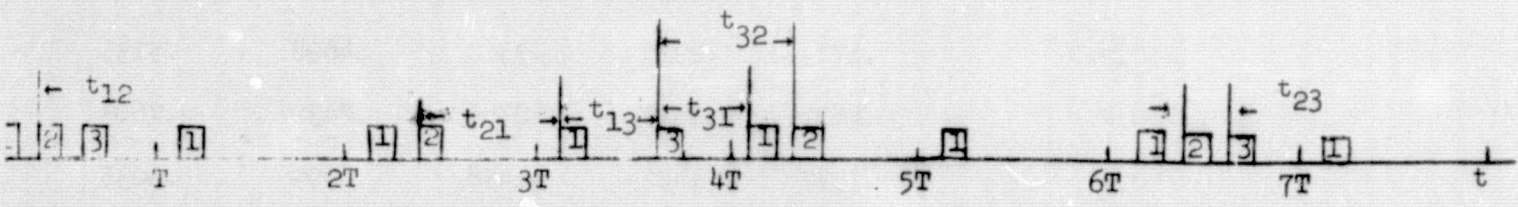
PARAMETERS	IRREDUNDANT SYSTEM RELIABILITY	$R_1(t)$	$R_2(t)$ r = 0	$R_2(t)$ r = 1	TOTAL r = 0	TOTAL r = 1
C = 1	0.2	.1773	.4387	.5134	.6160	.6901
δ = 1	0.4	.4817	.3923	.4215	.8740	.9032
	0.6	.7577	.2133	.2195	.9701	.9772
	0.8	.9388	.0585	.0588	.9973	.9976
	0.9	.9848	.0149	.0149	.9997	.9997
C = 0.9	0.2	.1592	.3511	.4040	.5103	.5632
δ = 1	0.4	.4417	.3171	.3378	.7588	.7795
	0.6	.7114	.1743	.1787	.8857	.8901
	0.8	.9064	.0484	.0486	.9548	.9550
	0.9	.9666	.0124	.0124	.9790	.9790
C = 1	0.2	.1773	.2925	.3360	.4698	.5133
δ = 0	0.4	.4817	.2615	.2786	.7432	.7603
	0.6	.7577	.1422	.1458	.8999	.9035
	0.8	.9388	.0390	.0392	.9778	.9780
	0.9	.9848	.0099	.0100	.9947	.9948

To illustrate the use of the coverage model, consider a set of three software tests and two hardware detectors designed to detect faults in a given category. Let the three software tests have detection probabilities P_i, $i = 1, 2, 3$, and detection rates,

$$i_i(\tau) = \begin{cases} \dfrac{1}{\Delta t_i} & 0 \le \tau \le \Delta t_i \\ 0 & \text{Otherwise} \end{cases} \qquad i = 1, 2, 3$$

Further, let test 1 be run every minor cycle (i.e. every T seconds), test 2 every other minor cycle, and test 3 every third minor cycle, and let them be scheduled as shown in Figure 3 . Then, with reference to equation 15, we have $n_1 = 1$, $n_2 = 2$, $n_3 = 3$, $n_c = \text{lcm}\,(1, 2, 3) = 6$. It is convenient to assume that the time separation between the i^{th} and j^{th} software tests exceeds the duration of both (i.e. that $t_{ij} \ge \Delta t_i + \Delta t_j$) since this condition considerably simplifies the resulting expressions for $g_i'(\tau)$.

FIGURE 3
DIAGNOSTIC TEST SCHEDULES



Making this assumption, defining

$$\rho_{ij}(\tau) = \begin{cases} 1 & \tau \le t_{ij} - \Delta t_i \\ 1 - \frac{P_i}{2}\left(\frac{\tau - (t_{ij} - \Delta t_i)}{\Delta t_i}\right)^2 & t_{ij} - \Delta t_i \le \tau \le t_{ij} \\ 1 - P_i + \frac{P_i}{2}\left(\frac{\tau - (t_{ij} + \Delta t_i)}{\Delta t_i}\right)^2 & t_{ij} \le \tau \le t_{ij} + \Delta t_i \\ 1 - P_i & t_{ij} + \Delta t_i \le \tau \end{cases}$$

and letting $\rho_{ij}'(\tau)$ be similiarly defined but with t_{ij} replaced everywhere by $t_{ij} + T$, we can carry out the integration in equation 15 obtaining:

$$g_1'(\tau) = \begin{cases} \frac{1}{6T}\left(2 + \rho_{31}(\tau)\right)\left(1 + \rho_{21}(\tau)\right) & 0 < \tau < T \\ 0 & T < \tau \end{cases}$$

$$g_2'(\tau) = \begin{cases} \frac{1}{6T}\rho_{12}(\tau)\left(1 + \rho_{32}(\tau) + \rho_{32}'(\tau)\right) & 0 < \tau < 2T \\ 0 & 2T < \tau \end{cases}$$

and

$$g_3'(\tau) = \begin{cases} \frac{1}{6T}\rho_{13}(\tau)\left(\rho_{23}(\tau) + \rho_{23}'(\tau)\right) & 0 < \tau < 3T \\ 0 & 3T < \tau \end{cases}$$

Now suppose the two hardware detectors can both be modeled as impulse detectors, one with a detection delay of t_4 seconds and the second with a t_5 second delay. It then follows from equation 16, that:

$$g_i(\tau) \quad i = 1, 2, 3 = \begin{cases} g_i'(\tau) & 0 < \tau < t_4 \\ (1 - P_4)\, g_i'(\tau) & t_4 < \tau < t_5 \\ (1 - P_4)(1 - P_5)\, g_i'(\tau) & t_5 < \tau < n_i T \end{cases}$$

$$g_4(\tau) = \left\{1 - \sum_{j=1}^{3} P_j \int_0^{t_4} g_j'(\eta)\, d\eta\right\} \delta(\tau - t_4)$$

$$g_5(\tau) = (1 - P_4)\left\{1 - \sum_{j=1}^{3} P_j \int_0^{t_5} g_j'(\eta)\, d\eta\right\} \delta(\tau - t_5)$$

with $\delta(t)$ the Dirac delta function.

Suppose further that the isolation procedure associated with each of these detectors requires exactly τ_d seconds (i.e. $h_i(\tau) = \delta(\tau - \tau_d)$, all i), that the amount of time needed to test a spare is τ_s seconds, and that total recovery is possible if and only if the fault is both detected and isolated within τ_r seconds of its occurrence (i.e. $r_i(\tau, \tau') = 1 - u(\tau + \tau' - \tau_r)$ with $u(\tau)$ a unit step function: $u(\tau) = 0$, $\tau < 0$; $u(\tau) = 1$, $\tau > 0$). Then, from equation 14, we have:

$$C_{ik} = P_i\, P_i'\, P''^{k} \int_0^{\infty} g_i(\tau) \int_0^{\infty} \delta(\tau' - k\tau_s - \tau_d)\left[1 - u(\tau + \tau' - \tau_r)\right] d\tau' d\tau$$

$$= P_i\, P_i'\, P''^{k} \int_0^{T_s = \tau_r - \tau_d - k\tau_s} g_i(\tau)\, d\tau$$

Although we could continue with this example at the present level of generality, the results are more readily interpretable if we add some additional constraints. In particular,

$$P_1 = P_2 = P_3 = P_4 = P_5 = P$$

$$P' = P''$$

$$t_{12} = t_{23} = t_{31} = T/3$$

$t_4 = T/4$

$t_5 = T/2$

$\tau_r = 3T/2$

$\tau_d = T/4$

$\tau_s = T/4$

The above expression for C_{ik} then becomes:

$$C_{11} = P\left(1 - \frac{22}{3?} P + \frac{23}{18} P^2 - 4/9\, P^3 + \frac{1}{18} P^4\right)$$

$$C_{12} = P\left(3/4 - \frac{67}{72} P + \frac{41}{72} P^2 - \frac{11}{72} P^3 + \frac{1}{72} P^4\right)$$

$$C_{21} = P/2\left(1 - \frac{73}{36} P + 2\, P^2 - 5/6\, P^3 + \frac{1}{9} P^4\right)$$

$$C_{22} = P/2\left(3/4 - \frac{43}{36} P + P^2 - 1/3\, P^3 + 1/36\, P^4\right)$$

$$C_{31} = P/6\left(2 - \frac{23}{?} P + \frac{23}{6} P^2 - \frac{11}{6} P^3 + \frac{1}{3} P^4\right)$$

$$C_{32} = P/6\left(3/ - \frac{25}{12} P + \frac{19}{12} P^2 - \frac{7}{1?} P^3 + \frac{1}{12} P^4\right)$$

$$C_{41} = C_{42} = P\left(1 - \frac{11}{24} P\right)$$

$$C_{51} = C_{52} = P\left(1 - P\right)\left(1 - \frac{11}{12} P + 1/6\, P^2\right)$$

Numerical values of these coverage coefficients are tabulated in Table 4 as a function of the probability P that any one of the detectors would by itself eventually detect the fault in the absence of any competition.

TABLE 4

COVERAGE COEFFICIENTS

P	k	C_{1k}	C_{2k}	C_{3k}	C_{4k}	C_{5k}	C_{tot}	$\delta = C^2/C^1$
1	1	.2500	.1250	.0833	.5417	0	1.0000	
1	2	.2500	.1250	.0833	.5417	0	1.0000	1.0000
.99	1	.2495	.1242	.0831	.5408	.0025	1.0000	
.99	2	.2494	.1242	.0831	.5408	.0025	1.0000	1.0000
.95	1	.2474	.1210	.0819	.5364	.0133	1.0000	
.95	2	.2472	.1209	.0819	.5364	.0133	0.9997	0.9997
.90	1	.2452	.1172	.0806	.5288	.0279	.9997	
.90	2	.2443	.1171	.0805	.5288	.0279	.9986	0.9989
.80	1	.2415	.1106	.0779	.5067	.0597	.9964	
.80	2	.2380	.1101	.0776	.5067	.0597	.9921	0.9957
.60	1	.2327	.1013	.0727	.4350	.1224	.9641	
.60	2	.2193	.0974	.0705	.4350	.1224	.9446	.9798
.40	1	.2087	.0917	.0647	.3267	.1584	.8502	
.40	2	.1838	.0823	.0590	.3267	.1584	.8102	.9530
.20	1	.1440	.0670	.0458	.1817	.1317	.5702	
.20	2	.1171	.0548	.0381	.1817	.1317	.5234	.9179

Several observations can be made concerning this particular example. It will be noted, for example, that the hardware detector having the T/4-second detection delay is generally the most effective device although its advantage decreases with decreasing P. The relative effectiveness of the software diagnostic programs is highly correlated to the frequency with which these programs are run and is comparatively independent of the order in which they are scheduled. These conclusions, however, are strongly influenced by the fact that the detection and isolation procedures must be completed in a relatively short time in this example for the recovery process to be successful.

V. EXTENSION TO THREE AND MORE MODES

The CARE II reliability model can readily be extended to include three or more modes of operation although the complexity of the resulting analytical expressions increases correspondingly. (The CARE II coverage model allows coverage to be determined as a function of the mode of operation, so it already is sufficient to model an arbitrary number of modes.) This increased complexity is due in part to the fact that two or more mode changes are now possible and in part to the increased number of ways in which this sequence of mode changes can be instigated. (E.g. a spares depletion in stage i could cause a change from mode 1 to mode 2 followed by a spares depletion in stage j causing a degeneration to mode 3 with both $i = j$ and $i \neq j$ as distinct possibilities.) Nevertheless, the appropriate reliability expressions are straightforward extensions of these described in Section II.

Consider first the case of three modes. In analogy with the category two and category three failures defined earlier, let a category three failure be redefined as a failure that, by itself, prevents operation in mode 1 or 2 but not in mode 3, and let a category four failure be one precluding all operation (i.e., a single-point failure for the three-mode system). Then the reliability of the three-mode configuration can be written:

$$R(t) = \left(R_1(t) + R_2(t) + R_3(t)\right)e^{-\lambda_4 t} \qquad (18)$$

with $R_1(t)$ and $R_2(t)$ exactly as defined in Section II, $R_3(t)$ the probability that the system survives until time t having degenerated to mode 3 sometime prior to t, and $e^{-\lambda_4 t}$ the probability that no category four failures, occurring at a rate λ_4 failures per unit time, have taken place by time t.

Since expressions for $R_1(t)$ and $R_2(t)$ have already been derived it remains only to determine $R_3(t)$. To this end we observe that there are six mutually exclusive categories of fault sequences that can result in a degeneration to mode 3: (1) A fault in stage x causes degeneration to mode 2 and a subsequent fault in stage z causes degeneration to mode 3, with $x \neq z$. (2) The previous fault sequence takes place but with $x = z$. (3) A category two fault causes degeneration to mode 2 and a subsequent failure in stage x causes degeneration to mode 3. (4) A failure in stage x causes degeneration to mode 2 and a category three failure causes degeneration to mode 3. (5) A category two failure causes degeneration to mode 2 and a category three failure causes degeneration to mode 3. (6) A category three failure forces the system to degenerate directly from mode 1 to mode 3. (It is implicitly assumed by this verbal description that the number of operational units required for any stage in mode i is at least one greater than that required for operation in mode j for $i < j$. Thus, no single failure in any stage can by itself cause degeneration from mode 1 to mode 3. The expressions to be derived, however, will remain valid even if this assumption is violated provided the proper limiting conditions are observed.)

Let $T_{3i}(t)$ denote the probability that the i^{th} event itemized in the previous paragraph actually takes place. Then:

$$R_3(t) = \sum_{i=1}^{6} T_{3i}(t) \tag{19}$$

In order to derive expressions for the $T_{3i}(t)$ terms, it is convenient to define some additional terms analogous to those used in Section II. Specifically, let

$$U_x(\tau_1, \tau_2, t) =$$

$$\sum_{j=0}^{r_1} \sum_{i=0}^{j} H_{x1}(\tau_1)\, G_{x2}(r_1 - j, \tau_2 - \tau_1) \binom{j}{i} \left(1 - e^{-\mu_x(\tau_2 - \tau_1)}\right)^{j-i} e^{-i\mu_x(\tau_2 - \tau_1)} \times$$

$$\times R_{x3}(i', t - \tau_2) \tag{20}$$

$$V_x(\tau_1, \tau_2, t) =$$

$$\sum_{j=0}^{S_x} \sum_{k=0}^{S_x - j} G_{x1}(j, \tau_1) \binom{S_x - j}{k} (1 - e^{-\mu_x \tau_1})^{S_x - j - k} e^{-k\mu_x \tau_1} H_{x,2}(k', \tau_2 - \tau_1) \times$$

$$\times R_{x3}(r_2, t - \tau_2) \tag{21}$$

$$W_x(\tau_1, \tau_2, t) = H_{x1}(\tau_1)\, H_{x2}(r_1, \tau_2 - \tau_1)\, R_{x3}(r_2, t - \tau_2) \tag{22}$$

and let

$$S_x(\tau_1, \tau_2, t) = \sum_{j=0}^{S_x} \sum_{k=0}^{S_x - j} G_{x1}(j, \tau_1) \binom{S_x - j}{k} (1 - e^{-\mu_x \tau_1})^{S_x - j - k} e^{-k\mu_x \tau_1} \times$$

$$\times \sum_{j=0}^{k'} \sum_{i=0}^{k'-j} G_{x2}(j, \tau_2 - \tau_1) \binom{k' - j}{i} (1 - e^{-\mu_x(\tau_2 - \tau_1)})^{k' - j - i} \times \tag{23}$$

$$\times e^{-i\mu_x(\tau_2 - \tau_1)} R_{x3}(i', t - \tau_2)$$

These expressions denote the probability (density) that stage x survives in mode 1 and until time τ_1, in mode 2 until time τ_2 and in mode 3 until time t. They differ in that $U_x(\tau_1, \tau_2, t)$ represents the case in which the first mode change is due to a depletion of spares in stage x itself, $V_x(\tau_1, \tau_2, t)$ the case in which x causes the second mode change, $W_x(\tau_1, \tau_2, t)$ the case in which it causes both changes, and $S_x(\tau_1, \tau_2, t)$ the case in which neither of the changes is due to a spares deficiency in stage x. These expressions are entirely analogous to those described in Section II. As there, these expressions also assume that all spares not already known to be defective are tested at each mode change. The terms $H_{x\ell}(\tau)$, $G_{x\ell}(i, \tau)$, $R_{x\ell}(i, t)$ etc. are as defined in Section II (the second subscript refers to the mode), and $H_{x\ell}(i, \tau) = H_{x\ell}(\tau)$ with S_x replaced by i. (When $\ell = 2$ here, the coverage terms become C_x'' and δ_x'', the double "primes" indicating that the mode 2 to mode 3 transitional values of these terms are to be used.) Again, as in Section II, the "prime" on an integer indicates that this parameter is to be incremented as appropriate if active units are reassigned to the spares pool. (E.g. in the expression for $U_x(\tau_1, \tau_2, t)$, $i' = i$ if units are not reassigned and $i' = i + Q_{x2} - Q_{x3}$ if they are. Similarly, $k' = k + Q_{x1} - Q_{x2}$ in the expression for $V_x(\tau_1, \tau_2, t)$ if the active units of stage x are reassigned at the time τ_1, and $k' = k$ otherwise.) The parameter r_1 is also as previously defined and r_2 is the corresponding term when the transition is from mode 2 to mode 3: $r_2 = 0$ if units are not reassigned; $r_2 = Q_{x2} - Q_{x3} - 1$ if they are.

The probabilities $T_{31}(t)$ can now be expressed in terms of these functions:

$$T_{31}(t) = \int_0^t \int_0^{\tau_2} \sum_x \sum_{z \neq x} U_x(\tau_1, \tau_2, t)\, V_z(\tau_1, \tau_2, t) \prod_{y \neq x, z} S_y(\tau_1, \tau_2, t)\, e^{-\lambda_2 \tau_1}\, e^{-\lambda_3 \tau_2}\, d\tau_1\, d\tau_2$$

$$T_{32}(t) = \int_0^t \int_0^{\tau_2} \sum_x W_x(\tau_1, \tau_2, t) \prod_{y \neq x} S_y(\tau_1, \tau_2, t)\, e^{-\lambda_2 \tau_1}\, e^{-\lambda_3 \tau_2}\, d\tau_1\, d\tau_2$$

$$T_{33}(t) = \lambda_2 C_2 \sum_x \int_0^t \int_0^{\tau_2} \prod_{y \neq x} S_y(\tau_1, \tau_2, t)\, e^{-\lambda_2 \tau_1}\, V_x(\tau_1, \tau_2, t)\, e^{-\lambda_3 \tau_2}\, d\tau_1\, d\tau_2$$

$$T_{34}(t) = \lambda_3 C_3 \sum_x \int_0^t \int_0^{\tau_2} \prod_{y \neq x} S_y(\tau_1, \tau_2, t)\, U_x(\tau_1, \tau_2, t)\, e^{-\lambda_2 \tau_1}\, e^{-\lambda_3 \tau_2}\, d\tau_1 d\tau_2 \qquad (24)$$

$$T_{35}(t) = \lambda_2 \lambda_3 C_2 C_3 \int_0^t \int_0^{\tau_2} \prod_y S_y(\tau_1, \tau_2, t)\, e^{-\lambda_2 \tau_1}\, e^{-\lambda_2 \tau_2}\, d\tau_1\, d\tau_2$$

$$T_{36}(t) = \lambda_3 C_3 \int_0^t \prod_y S_y(\tau_1, \tau_1, t)\, e^{-\lambda_2 \tau_1}\, e^{-\lambda_3 \tau_1}\, d\tau_1$$

The extension to four and more modes is straightforward but the resulting expressions become correspondingly more complex. For four modes the reliability assumes the form

$$R(t) = \left(R_1(t) + R_2(t) + R_3(t)\right) e^{-(\lambda_4 + \lambda_5) t} + R_4(t)\, e^{-\lambda_5 t} \qquad (25)$$

and for five modes

$$R(t) \left(R_1(t) + R_2(t) + R_3(t)\right) e^{-(\lambda_4 + \lambda_5 + \lambda_6) t} + R_4(t)\, e^{-(\lambda_5 + \lambda_6)} + R_5(t)\, e^{-\lambda_6 t} \qquad (26)$$

etc. The terms $R_1(t)$, $R_2(t)$, and $R_3(t)$ are as previously defined. The probability $R_4(t)$ involves twenty-two terms similar to the $T_{31}(t)$ terms just defined but with many of these terms triple integrals; $R_5(t)$ requires seventy-three such terms many of which are quadruple integrals.

While the CARE II program could in principle be extended to include more than two modes, it is apparent from the preceding discussion that the time required to calculate R(t) for any particular set of parameters is an exponentially increasing function of the number of modes allowed. If additional restrictions were imposed on the model, however, the time needed to complete a computation could be brought back to reasonable values. If, for example, it could be established that failures of category two and higher were sufficiently unlikely to be ignored, the complexity of the computation could decrease dramatically. Only two of the six $T_{31}(t)$ terms required in the evaluation of $R_3(t)$, for example,would remain; $R_4(t)$ would involve only five triple integrals and $R_5(t)$ fifteen quadruple integrals rather than the seventy-three previously mentioned. In addition, the number of terms would reduce still further (and the resulting terms would be simpler) if the number of stages comprising the computer system were restricted. (In the above discussion it was assumed that the number of stages was at least as great as the number of modes minus one (i.e. three stages in a 4-mode configuration, etc.) If only two stages were allowed, for example, the number of terms needed to evaluate $R_5(t)$ would be reduced further from fifteen to eight; and only one such term is required to model a single-stage system.

VI. CONCLUSIONS AND RECOMMENDATIONS

The CARE II program as it currently exists is an extremely versatile tool for modeling the reliability of a dual-mode computer system. The computer can be segregated into as many as eight different stages each with its own coverage parameters, active and dormant failure rates, and its own complement of spares. A mode change can result upon the exhaustion of spares in any stage or from the inability to operate in a dual mode even when adequate units are available at each stage (category two failures).

As discussed in Section V, the extension of this model to include systems capable of operating in three or more modes is conceptually straightforward. Unfortunately, the resulting computational time can become excessive unless some restrictions are placed on the generality of the model. Several possibilities were identified in this regard.

Two approaches suggest themselves for implementing this extended version of CARE II (with or without these additional restrictions). The obvious approach is to use the present CARE II to calculate $R_1(t)$ and $R_2(t)$ and augment it with new subroutines to determine $R_3(t)$, $R_4(t)$, etc. The major difficulty with this approach is the excessive time required to evaluate the resulting multiple integrals. (In general, an ℓ-mode model involves $(\ell-1)$-fold integrals.) An alternative approach using Laplace transforms to eliminate the need for any integration appears promising. Further investigation is needed to determine the ease with which the consequent inverse transforms can be evaluated by computer and to estimate the complexity of the resulting program as a function of the number of modes in the reliability model.

In any event, the extended program would consist primarily of a subroutine

for evaluating $R_1(t)$ with i the maximum number of modes likely ever to be required (e.g. i = 5). The terms $R_{i-1}(t)$, $R_{i-2}(t)$ could then be determined by repeatedly using this same subroutine with appropriate substitutions.

That is, suppose a subroutine were written to calculate:

$$R_3(t) = \sum_{i=1}^{6} T_{3i}(t)$$

with the $T_{3i}(t)$ terms as defined in equation 24. Then:

$$R_2(t) = \left(T_{31}'(t) + T_{33}'(t)\right) e^{-\lambda_3 t}$$

where $T_{3i}'(t) = T_{3i}(t)$ with $\sum_z V_z(r_1, r_2, t)$ replaced by $S_y(r_1, r_2, t)\,\delta(r_1 - \cdot\cdot$

Similar substitutions would yield $R_1(t)$ and the desired result would be obtained after three (or, in general, i) successive iterations using this same subroutine.

VII.

APPENDIX

A PROOF OF EQUATION 5

The recursion

$$G(m+1,t) = \sum_{i=0}^{m} \int_{0}^{t} KQ\mu \; G(i,\tau)\,(1-e^{-\mu\tau})^{m-i}\, e^{-\mu\tau}\, C\delta^{m-i}\, e^{-KQ\mu(t-\tau)}\, d\tau \quad (27)$$

follows directly from the definition of $G(i,t)$. That is, exactly $m+1$ spares are used by time t if a failure occurred in the infinitesimal time interval $(\tau, \tau + d\tau)$ (an event having probability $KQ\mu\, d\tau$), if exactly i spares had been used up to that point $(G(i,\tau))$, if the first $m-i$ spares tested are defective $((1-e^{-\mu\tau})^{m-i})$ but the $(m-i+1)^{st}$ spare is operational $(e^{-\mu\tau})$, if recovery is possible under these conditions $(C\delta^{m-i})$ and if the system survives for the remaining $t-\tau$ units of time without any additional failures $(e^{-KQ\mu(t-\tau)})$. Integrating the resulting probability density over all τ, $0<\tau<t$, yields the conditional probability that exactly $m+1$ spares are used given that $m-i+1$ spares had to be tested during recovery from the last failure in that interval. Since, for any $m \geq 0$, i must be an integer in the range $0 \leq i \leq m$, since these events are mutually exclusive for different integers i, and since at least one failure must have occurred for any $m \geq 0$, the sum of these probabilities over all i, $0 \leq i \leq m$, must equal $G(m+1,t)$.

Now assume that equation (5) is true for all $G(i,t)$ with $0 \leq i \leq m$. Then substituting this expression for $G(i,t)$ into equation (27) and rearranging terms, we obtain:

$$G(m+1,t) =$$

$$KQ\mu\, C \sum_{i=0}^{m} \binom{M+i-1}{i} \delta^{m} \int_{0}^{t} (1-e^{-\mu\tau})^{m}\, e^{-\mu\tau}\, d\tau\, e^{-KQ\mu t}$$

$$= KQC \binom{M+m}{m} \delta^{m} \frac{(1 - e^{-\mu t})^{m}}{m} e^{-KQ\mu t}$$

$$= \binom{M+m}{m+1} \delta^{m+1} (1 - e^{-\mu t})^{m+1} e^{-KQ\mu t}$$

Thus, since equation (5) is obviously true for i = 0, it is also true, by recursion, for all integers i > 0.